AMENDMENTS TO THE SPECIFICATION AND ABSTRACT

Please amend the paragraph beginning on page 4, lines 11-27 as follows:

The version 8001 is the version of this certificate revocation list. The signature algorithm 8002 indicates the algorithm used by the issuer in signing this certificate revocation list. The issuer 8003 indicates the name of the issuing CA of the CRL 8000. The update time 8004 is the date and time of issue of this certificate revocation list. The next update time 8005 is the date and time by which the certificate revocation list will be updated next time. The revoked certificate 8006 is a list of serial numbers ~~8006b~~8006a and revocation times ~~8006b~~ 8006a of respective revoked server certificates. Out of server certificates issued by the CA under the name of an issuer, the serial number of each server certificate judged to be invalid by the CA shall be described as a serial number 8006b, together with its revoked time 8006b. The signature algorithm 8007 is the algorithm used by the issuing CA in signing this certificate revocation list. And the signature 8008 is a signature created by the CA with its CA private key on the part in this CRL 8000 excluding such signature.

Please amend the paragraph beginning on page 8, lines 10-18 as follows:

The server certificate verification unit 4200 reads the validity period 7005 from the received server certificate 7000, and obtains the current time from the clock 4300 (S9051). Then, the server certificate verification unit 4200 compares the current time with the start and expiration dates of the validity period 7005 (S9052), and notifies the communication unit 4400 of an error code indicating period expiration, when the current time is not within the validity period 7005 of the server certificate 7000, so as to end the verification (S9057).

Please amend the paragraph beginning on page 8, lines 19-30 as follows:

Meanwhile, when the current time is within the validity period 7005 of the server certificate 7000, the server certificate verification unit 4200 reads the issuer 7004 from the server certificate 7000, and further searches the CA certificate storage unit 4210 for the CA certificate 6000 of such issuer 7004 (S9053). When there exists the CA certificate 6000 corresponding to the issuer 7004, the server certificate verification unit 4200 reads the CA public key from such CA certificate 6000, and checks the signature 7008 on the server certificate 7000 by use of the CA public key (S9054). When the signature 7008 is invalid, the server certificate verification unit 4200 notifies the communication unit 4400 of an error code indicating verification error, and ends the verification (S9057).

Please amend the paragraph beginning on page 8, line 31 to page 9, line 11 as follows:

When the signature 7008 is valid, the server certificate verification unit 4200 reads the serial number 7002 from the server certificate 7000 (S9055). Then, the server certificate verification unit 4200 reads the CRL 8000 from the CRL storage unit 4220, and checks whether such serial number 7002 is included in the CRL 8000 or not (S9056). When the CRL 8000 includes the serial number 7002, the server certificate verification unit 4200 judges that the server certificate 7000 is revoked, and notifies the communication unit 4400 of an error code indicating revocation, so as to end the verification (S9057). Meanwhile, when the CRL 8000 does not include the serial number 7002, the server certificate verification unit 4200 judges that the server certificate 7000 is valid, and notifies the communication unit 4400 that the verification has ended normally.

Please amend the sub-title on page 18, line 15 as follows:

~~Best Mode for Carrying Out~~ Detailed Description of the Invention

Please amend the paragraph on page 35, lines 18-32 as follows:

The revoked certificate search unit 113 waits for the server certificate validity period search unit 111 to notify the largest value ~~Seen~~ Se end of all the serial numbers to be actually revoked (S31). When notified of the largest value ~~Seen~~ Se end of the serial numbers to be actually revoked (Yes in S31), the revoked certificate search unit 113 notifies the certificate revocation notification unit 114 of the server names corresponding to the serial numbers from the smallest serial number Se min through to the largest serial value Se end (S32). Accordingly, the certificate revocation notification unit 114 sends a revocation notification 80 to each of the corresponding application servers 30a~30k. Then, each of the application servers 30a~30k that has received the revocation notification 80 sends a CSR 70, as a result of which a new server certificate 75 that is assigned a serial number that increments monotonously, is to be issued for each of such application servers 30a~30k.

Please amend the paragraph beginning on page 38, line 31 to page 39, line 3 as follows:

FIG. 16 is a flowchart showing the operation performed by each unit in the server certificate verification unit 430 when obtaining revocation information. Note that such processing is carried out regularly at predetermined time intervals (e.g., once a month).

Please amend the paragraph beginning on page 39, lines 4-12 as follows:

First, the revocation information request unit 431 of each of the terminals 40a~40n obtains the revocation information 90 from the repository 20 regularly (e.g., once a month), and stores the revocation number. More specifically, the revocation information request unit 431 waits for a month to pass according to the internal timer (S61). When a month has passed (Yes in S61), the revocation information request unit 431 requests the repository 20 to distribute revocation information 90 (S62), and waits for the revocation information 90 to be distributed (S63).

Please amend the paragraph beginning on page 47, line 27 to page 48, line 4 as follows:

Moreover, since a server certificate 75 to be issued is assigned a serial number which increments monotonously, with the default serial number of a server certificate 75 being set to a value equal to or larger than the default revocation number, it is possible to enjoy the functionality equivalent to the one to be achieved when the revocation serial number is referred to, which is why the revocation number is not used as a reference in the present embodiment. However, the revocation number may be actually ~~refereed~~ referred to, so as to issue a server certificate 75 with a serial number that is equal to or larger than such revocation number.

Please amend the paragraph beginning on page 52, lines 9-21 as follows:

Each of the terminals 41a~41n is made up of the application client unit 410, a communication unit 440 instead of the communication unit 420, and a server certificate verification unit 450 instead of the server certificate verification unit 430. The server certificate verification unit 450 is made up of the signature verification unit 432, the CA certificate storage unit 433, the revocation number storage unit 436, and the revocation judgment unit 438, as in the case of the server certificate verification unit 430, and further includes a revocation information request unit 451 ~~in stead~~ instead of the revocation information request unit 431, a certificate serial number extraction unit 452 instead of the certificate serial number extraction unit 437, and a revocation number verification unit 453 instead of the revocation number verification unit 435.

Please amend the paragraph beginning on page 56, line 27 to page 57, line 8 as follows:

Moreover, said server certificate issuing apparatus (1) searches the server certificate information storage unit for a server certificate whose validity period is approaching, so as to obtain the identification number of said server certificate, (2) determines, as a new revocation number, a number which is larger than said identification number, (3) stores said new revocation number into the revocation number storage unit, (4) searches the server certificate information storage unit so as to read ~~o ut~~ out a server certificate (hereinafter referred to as “a server certificate to be renewed”) whose identification number is equal to or smaller than the identification number of the server certificate, and (5) issues, to a server which possesses said server certificate to be renewed, a new server certificate whose identification number is equal to or larger than the new revocation number.

Please amend the Abstract as follows:

A terminal ~~(40a) comprises:~~includes (i) a revocation number verification unit ~~(435)~~ that obtains a revocation number from a repository ~~(20)~~ storing ~~such~~ the revocation number that is information serving as a criterion for judging the validity of a server certificate ~~(75);~~, (ii) a revocation number storage unit ~~(436)~~ that stores the obtained revocation number~~;~~, (iii) a certificate serial number extraction unit ~~(437)~~ that reads out, from the server certificate ~~(75)~~, an identification number for identifying such server certificate ~~(75);~~, and (iv) a revocation judgment unit ~~(438)~~ that judges the validity of the server certificate ~~(75) by~~by comparing the read-out identification number with the revocation number stored by the revocation number storage unit ~~(436);~~. ~~and~~ The terminal further includes a communication unit ~~(420)~~ that establishes a communication with an application server ~~(30a)~~ when the server certificate ~~(75)~~ is judged to be valid, and does not establish a communication with the application server ~~(30a)~~ when the server certificate ~~(75)~~ is judged to be invalid.